2004 Security Costs Estimates Display

Name of Department/Agency: Peace Corps

Reporting Categories	FY 2002 (Est in $000)	FY 2003 (Est in $000)	FY 2004 (Est in $000)
1. Personnel Security	153.2	159.6	164.3
2. Physical Security	1	1	1
3. Information Security (Sum of a, b & c below)	.5	.5	.5
a. Classification Management	.5	.5	.5
b. Declassification	0	0	0
c. Information Technology (Electronic Security)	0	0	0
4. Professional Education, Training, and Awareness	2.9	3.1	3.3
5. Security Management, Oversight, and Planning	8.3	8.5	8.6
6. Unique Items	0	0	0
Totals: Fiscal Year Estimates	~~166.4~~ 165.9	~~175.2~~ 172.7	~~178.2~~ 177.7
Totals: Full-Time Equivalents (FTE)	(2.73)	(2.55)	(2.5)

Narrative: Peace Corps does not have original classification authority.

David Dalton, the Director of the Office of Personnel Security, is the Point of Contact for this report. Please call him on (202) 692-1211, if you have any questions. (Future requests should be addressed to him at 1111 20th Street, Room 2307, Washington, DC 20526).

March 11, 2004

Ms. Laura L.S. Kimberly
Associate Director for Policy
Information Security Oversight Office
National Archives and Records Administration
Washington, DC 20408

Dear Ms. Kimberly

This is in response to your letter of February 2, 2004, requesting information on cost estimates for security classification activities. The enclosure reflects the estimated costs for the Peace Corps.

If further information is needed, please call David Dalton, Chief of Information and Personnel Safety and Security, on 692-1211.

Sincerely,

Patrick J. Hogan
Associate Director for Safety and Security

Enclosure

MAR 2 2 2004

BY:

2005 Security Costs Estimates Display

Name of Department/Agency: Peace Corps

Reporting Categories	FY 2003 (Est in $000)	FY 2004 (Est in $000)	FY 2005 (Est in $000)
1. Personnel Security	159.6	165.1	171.9
2. Physical Security	1	1	1
3. Information Security (Sum of a, b & c below)	.5	.6	.65
a. Classification Management	.5	.6	.65
b. Declassification	0	0	0
c. Information Technology (Electronic Security)	0	0	0
4. Professional Education, Training, and Awareness	3.1	3.4	3.6
5. Security Management, Oversight, and Planning	8.5	8.6	8.7
6. Unique Items	0	0	0
Totals: Fiscal Year Estimates	~~173.2~~ 172.7	179.3	186.5
Totals: Full-Time Equivalents (FTE)	(2.55)	(2.65)	(3.0)

Narrative: Peace Corps does not have original classification authority.

David Dalton, the Chief of the Office of Information and Personnel Safety and Security, is the Point of Contact for this report. Please call him on (202) 692-1211, if you have any questions.

Peace Corps

April 27, 2005

Mr. J. William Leonard
Director
Information Security Oversight Office
National Archives and Records Administration
Washington, DC 20408

Dear Mr. Leonard:

Please find attached the 2006 Security Costs Estimates
Display for Peace Corps.

If any additional information is needed, please call David
Dalton, Chief, Information and Personnel Safety and
Security Division, at (202) 692-2559 or Joseph Jaffa, at 692-
2554.

Sincerely,

Patrick J. Hogan
Associate Director for Safety & Security

2006 Security Costs Estimates Display

Name of Department/Agency: Peace Corps

Reporting Categories	FY 2004	FY 2005	FY 2006
1. Personnel Security	337,300	349,899	362,987
2. Physical Security	1,000	1,100	1,250
3. Information Security	600	650	675
(a.) Classification Management	600	650	675
(b.) Declassification	0	0	0
(c.) Information Systems Security for Classified Information	0	0	0
(d.) Miscellaneous (OPSEC & TSCM)	0	0	0
(e.) Information Security Subtotal (Sum of 3.a, 3.b, 3.c, & 3.d)	600	650	675
4. Professional Education, Training, and Awareness	3,500	3,600	3,675
5. Security Management, Oversight, and Planning	8,858	9,221	9,548
6. Unique Items	0	0	0
Totals: Fiscal Year Estimates	~~351,858~~* 351,258	365,120	378,810

NARRATIVE:

Peace Corps does not have original classification authority.

* Figures include cost of contract investigators' field investigations on candidates for security clearances which were not included in prior years.

David Dalton, Chief, Information and Personnel Safety and Security Division, is the point of contact for this report. He can be reached at (202) 692-2559.

45th

Peace Corps
Anniversary

1961-2006: a leg↑ · of service at home and abroad

Rec'd - Andrc

APR - 7 2006

April 5, 2006

Mr. J. William Leonard
Director
Information Security Oversight Office
National Archives and Records Administration
Washington, DC 20408

Dear Mr. Leonard:

Please find attached the 2007 Security Costs Estimates
Display for Peace Corps.

If any additional information is needed, please call David
Dalton, Chief, Information and Personnel Safety and
Security Division, at (202) 692-2559 or Joseph Jaffa, at 692-
2554.

Sincerely,

Patrick J. Hogan
Associate Director for Safety & Security

2007 Security Costs Estimates Display

Name of Department/Agency: **Peace Corps**

Reporting Categories	FY 2005	FY 2006	FY 2007
1. Personnel Security	349,000	362,000	375,000
2. Physical Security	1,100	1,200	1,300
3. Information Security	~~650~~	675	700
(a.) Classification Management	650	675	700
(b.) Declassification	0	0	0
(c.) Information Systems Security for Classified Information	0	0	0
(d.) Miscellaneous (OPSEC & TSCM)	0	0	0
(e.) Information Security Subtotal (Sum of 3.a, 3.b, 3.c, & 3.d)	~~650~~	675	700
4. Professional Education, Training, and Awareness	3,600	3,700	3,800
5. Security Management, Oversight, and Planning	9,200	9,500	9,800
6. Unique Items	0	0	0
Totals: Fiscal Year Estimates	~~364,750~~ 363,550	378,325	391,950

NARRATIVE:

Peace Corps does not have original classification authority.

David Dalton, Chief, Information and Personnel Safety and Security Division, is the point of contact for this report. He can be reached at (202) 692-2559.

45th
Peace Corps
Anniversary

1961-2006: a legacy (˜ervice at home and abroad

Red
4/9/07

April 2, 2007

Mr. J. William Leonard
Director
Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, NW, Room 503
Washington, DC 20408

Dear Mr. Leonard:

Please find attached the Security Costs Estimates Display for Peace Corps.

If further information is needed, call David Dalton, Chief of Information & Personnel Safety and Security, at (202) 692-2559 or Joseph Jaffa, at 692-2554.

Sincerely,

Patrick J. Hogan
Associate Director for Safety & Security

Security Costs Estimates Display

Name of Department/Agency: PEACE CORPS

Reporting Categories	FY 2006
1. Personnel Security	$361,600
2. Physical Security	$1,200
3. Information Security	////////////////////////////
(a.) Classification Management	$675
(b.) Declassification	0
(c.) Information Systems Security for Classified Information	0
(d.) Miscellaneous (OPSEC & TSCM)	0
(e.) Information Security Sub-Total (Sum of 3.a., 3.b., 3.c., & 3.d.)	$675
4. Professional Education, Training and Awareness	$3,700
5. Security Management, Oversight and Planning	$9,500
6. Unique Items	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(e.), 4, 5, & 6.)	$376,675

NARRATIVE:

Personnel Security – Costs include proportionate salaries of the Chief, two Personnel Security Specialists, one expert/consultant and a nationwide staff of contract investigators.

Peace Corps does not have original classification authority.

David Dalton, Chief, Information and Personnel Safety and Security Division, is the contact for this report. He can be reached at (202) 692-2559.
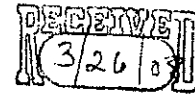
March 25, 2008

Mr. William J. Bosanko
Acting Director
Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, NW, Room 503
Washington, DC 20408

Dear Mr. Bosanko:

Please find attached the Security Costs Estimates Display for Peace Corps.

If further information is needed, call David Dalton, Chief of Information & Personnel Safety and Security, at (202) 692-2559 or Joseph Jaffa, at (202) 692-2554.

Sincerely,

David M. Dalton
Acting Associate Director for Safety & Security

Security Costs Estimates Display

Name of Department / Agency: Peace Corps

(Please use actual dollar figures instead of thousands)

Reporting Categories	FY 2007
1. Personnel Security	380,245
2. Physical Security	1,300
3. Information Security	
(a.) Classification Management	695
(b.) Declassification	0
(c.) Information Systems Security for Classified Information	0
(d.) Miscellaneous (OPSEC & TSCM)	0
(e.) Information Security Sub-Total (Sum of 3.a., 3.b., 3.c., & 3.d.)	695
4. Professional Education, Training and Awareness	3,700
5. Security Management, Oversight and Planning	9,800
6. Unique Items	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(e.), 4, 5, & 6.)	395,740

NARRATIVE:

Personnel Security—Costs in this area include proportionate salaries of the Chief, two Personnel Security Specialists, one expert/consultant and a nationwide staff of contract investigators.

Peace Corps does not have original classification authority.

David Dalton, the Chief of the Office of Information and Personnel Safety and Security, is the Point of Contact for this report and can be reached on (202) 692-2559.

Security Costs Estimates Display

Name of Department/Agency: Peace Corps

(Please use actual dollar figures instead of thousands)

Reporting Categories	FY 2008
1. Personnel Security	397,629
2. Physical Security	1,300
3. Information Security	
(a.) Classification Management	716
(b.) Declassification	0
(c.) Information Systems Security for Classified Information	0
(d.) Miscellaneous (OPSEC & TSCM)	0
4. Professional Education, Training and Awareness	3,700
5. Security Management, Oversight and Planning	10,100
6. Unique Items	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(a,b,c,d), 4, 5, & 6)	413,445

NARRATIVE: (Example)

Personnel Security—Costs in this area include proportionate salaries of the Chief, two Personnel Security Specialists, one expert/consultant and a nationwide staff of contract investigators.

Peace Corps does not have original classification authority.

David Dalton, the Chief of Domestic Operations, Office of Safety and Security, is the Point of Contact for this report and can be reached on (202) 692-2559

Security Costs Estimates Display

Name of Department/Agency: Peace Corps

(Please use actual dollar figures instead of thousands)

Reporting Categories	FY 2009
1. Personnel Security	284,280
2. Physical Security	28,524
3. Information Security	
(a.) Classification Management	1,200
(b.) Declassification	0
(c.) Information Systems Security for Classified Information	32,000
(d.) Miscellaneous (OPSEC & TSCM)	0
4. Professional Education, Training and Awareness	5,600
5. Security Management, Oversight and Planning	10,100
6. Unique Items	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(a b c,d), 4, 5, & 6)	361,704

NARRATIVE:

Personnel Security—Costs in this area have decreased as a result of downsizing throughout the Department. A recent review of security clearances resulted in a significant decrease in the number of employees holding clearances.

Physical Security/Information Security – Cost in these areas have increased as a result of the acquisition of systems equipment.

Peace Corps does not have original classification authority. Normally Peace Corps does not create any derivatively classified documents.

David Dalton, Chief, Domestic Operations, Office of Safety and Security, is the Point of Contact for this report and can be reached on (202) 692-2559.

Security Costs Estimates

Department/Agency:	Peace Corps	Fiscal Year:	2010

Point of Contact:
(Name and phone number) | Nicki Casteel, Chief, Information and Personnel Security (202) 692-2553

Reporting Categories

(Please use actual dollar figures instead of thousands)

1. Personnel Security

$365,099.00

(include clearance program, initial investigations, national agency checks when used for basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification related activities)

2. Physical Security

$39,067.00

(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification related activities)

3. Information Security

(only report costs associated with classification related activities)

(a) Classification Management

$1,236.00

(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)

(b) Declassification

$0.00

(include resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive order or statute)

(c) Information Systems Security for Classified Information

$32,000.00

(include resources used to protect information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)

(d) Miscellaneous (OPSEC and TSCM)

$0.00

(include personnel and operating expenses associated with these programs)

4. Professional Education, Training, and Awareness

$8,400.00

(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification related activities)

5. Security Management, Oversight, and Planning

$10,400.00

(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))

6. Unique Items

$0.00

(include department/agency-specific activities not reported in any of the categories listed above but are nonetheless significant and need to be included)

Total (sum of 1, 2, 3(a), 3(b), 3(c), 3(d), 4, 5, and 6)

$456,202.00

Narrative: *provide a brief explanation of any significance difference between last year's and this year's cost estimates. Explain items entered into Block 6. Unique Items.*

Increase in Personnel Security costs due to hiring of additional staff; increase in hourly pay rate for contract investigators; and increases amount of SSBI case types. Increase in Physical Security costs due to acquiring Dept. of State's ClassNet system. Increase in Professional Eduction, Training, and Awareness due to an increase in office direct hire staff participating in OPM's off-site Basic Investigation Course.

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Information Security with subcategories: Classification Management, Declassification, Information Systems Security for Classified Information, and Miscellaneous; (4) Professional Education, Training and Awareness (Education and Training); (5) Security Management, Oversight, and Planning (General Security); and (6) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information.) Counterintelligence* resources should also not be included in this data collection. All resources devoted to a classification-related activity should be included in this estimate; however, resources devoted on a part-time basis may be factored out of the estimate if the total time devoted to those activities during the course of the fiscal year is less than 51%. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information.)

1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

    Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

    Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

    National Agency Check: Include only when used for basis for granting a clearance.

    Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

    Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

    Polygraph: Substantive examinations in security screening process.

2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

    Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

    Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

    Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

    Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

    Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

    Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

    Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 C.F.R. 970.0404-1)

3. **Information Security:**

Classification Management: The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive order or statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

Declassification: The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive order or statute.

Information Systems Security for Classified Information: An information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats.

Other pertinent definitions under this subcategory:

Information Systems Security Engineering (ISSE): Process that captures and refines information protection requirements and ensures their integration into information technology acquisition processes through purposeful security design or configuration.

Information Systems Security Equipment Modification: Modification of any fielded hardware, firmware, software, or portion thereof, under National Security Agency configuration control. There are three classes of modifications: mandatory (to include human safety); optional/special mission modifications; and repair actions. These classes apply to elements, subassemblies, equipment, systems, and software packages performing functions such as key generation, key distribution, message encryption, decryption, authentication, or those mechanisms necessary to satisfy security policy, labeling, identification, or accountability.

TEMPEST: Short name referring to investigation, study, and control of compromising emanations from information systems equipment.

Communications Security (COMSEC): Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

Miscellaneous:

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

4. **Professional Education, Training, and Awareness:** The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

5. **Security Management, Oversight, and Planning:** Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create a SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

6. **Unique Items:** Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the six categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. **Name of Department/Agency.** Self-explanatory.

2. **Reporting Categories:** List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. **Totals:** Add the totals for blocks 1, 2, 3(a), 3(b), 3(c), 3(d), 4, 5, and 6 and place in the appropriate block.

4. **Narrative:** In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Peace Corps | **Fiscal Year:** 2011

Point of Contact:
(Name and phone number) Nicki Whitaker, Chief, Information and Personnel Security (202) 692-2553

Reporting Categories

Please use actual dollar figures.

1. Personnel Security
(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)

$400,735.48

2. Physical Security
(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)

$40,000.00

3. Classification Management
(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)

$0.00

4. Declassification
(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)

$0.00

5. Protection and Maintenance for Classified Information Systems
(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)

$33,500.00

6. Operations Security and Technical Surveillance Countermeasures
(include personnel and operating expenses associated with OPSEC and TSCM)

$0.00

7. Professional Education, Training, and Awareness
(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)

$0.00

8. Security Management, Oversight, and Planning
(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))

$0.00

9. Unique Items
(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)

$0.00

TOTAL
(sum of items 1-9)

$474,235.48

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

Our professional education, training and awareness costs have significantly decreased since we use the intranet as a means of training agency personnel regarding proper handling of classified, etc. In addition, due to budget restrictions, our staff has not been able to take formal training. Therefore, we have utilized cost free online courses.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION   AUTHORIZED FOR LOCAL REPRODUCTION   STANDARD FORM 716 (07-11)
Page 1 of 4   Prescribed by NARA/ISOO
32 CFR Part 2001.90 E.O. 13526

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Peace Corps	**Fiscal Year:** 2012

Point of Contact:
(Name and phone number) Nicki Whitaker, Chief, Information and Personnel Security (202) 692-2553

Reporting Categories

Please use actual dollar figures.

1. Personnel Security
(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)

$216,529.68

2. Physical Security
(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)

$2,000.00

3. Classification Management
(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)

$0.00

4. Declassification
(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)

$0.00

5. Protection and Maintenance for Classified Information Systems
(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)

$9,600.00

6. Operations Security and Technical Surveillance Countermeasures
(include personnel and operating expenses associated with OPSEC and TSCM)

$0.00

7. Professional Education, Training, and Awareness
(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)

$0.00

8. Security Management, Oversight, and Planning
(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))

$0.00

9. Unique Items
(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)

$0.00

TOTAL
(sum of items 1-9)

$228,129.68

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

Significant decreases from FY2011 totals are due to the following: the agency hired less employees/contractors which reduced the number of background investigations. HQ was renovated in FY2011 which required building new office space and a special room to house State Department's ClassNet terminal.

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. Report only those cost estimates associated with classification-related activities (programs that affect the security of classified information).

1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

   Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

   Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

   National Agency Check: Include only when used for basis for granting a clearance.

   Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

   Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

   Polygraph: Substantive examinations in security screening process.

2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

   Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

   Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

   Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

   Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Peace Corps	**Fiscal Year:** 2013

Point of Contact:
(Name and phone number) Nicki Whitaker, Chief, Information and Personnel Security (202) 692-2553

Reporting Categories

Please use actual dollar figures.

1. Personnel Security

(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)

$167,979.90

2. Physical Security

(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)

$1,073,089.78

3. Classification Management

(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)

$0.00

4. Declassification

(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)

$0.00

5. Protection and Maintenance for Classified Information Systems

(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)

$4,500.00

6. Operations Security and Technical Surveillance Countermeasures

(include personnel and operating expenses associated with OPSEC and TSCM)

$0.00

7. Professional Education, Training, and Awareness

(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)

$0.00

8. Security Management, Oversight, and Planning

(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))

$0.00

9. Unique Items

(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)

$0.00

TOTAL
(sum of items 1-9)

$1,245,569.68

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

Significant increase from FY2012 totals are due to the following: In years past, we did not include the cost of the guards for the headquarters building. The figure for FY 13 includes the cost of the headquarters guard contract.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION   AUTHORIZED FOR LOCAL REPRODUCTION   STANDARD FORM 716 (07-11)
Page 1 of 4   Prescribed by NARA/ISOO
32 CFR Part 2001.90 E.O. 13526

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified Information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

    1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

        Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

        Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

        National Agency Check: Include only when used for basis for granting a clearance.

        Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

        Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

        Polygraph: Substantive examinations in security screening process.

    2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

        Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

        Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

        Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

        Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION   AUTHORIZED FOR LOCAL REPRODUCTION   STANDARD FORM 716 (07-11)
Page 2 of 4   Prescribed by NARA/ISOO
32 CFR Part 2001.90 E.O. 13526

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. **Classification Management:** The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. **Declassification:** The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. **Protection and Maintenance for Classified Information Systems:** A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. **Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):**

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. **Professional Education, Training, and Awareness:** The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. **Security Management, Oversight, and Planning:** Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION AUTHORIZED FOR LOCAL REPRODUCTION STANDARD FORM 716 (07-11)
Page 3 of 4 Prescribed by NARA/ISOO
32 CFR Part 2001.90 E.O. 13526

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. **Unique Items:** Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. **Name of Department/Agency:** Self-explanatory.

2. **Reporting Categories:** List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. **Totals:** The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. **Narrative:** In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Peace Corps	Fiscal Year: 2014

Point of Contact:
(Name and phone number) Nicki Whitaker, Chief, Information and Personnel Security (202) 692-2553

Reporting Categories

Please use actual dollar figures.

1. Personnel Security
(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)

$231,682.80

2. Physical Security
(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)

$1,100,000.00

3. Classification Management
(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)

$0.00

4. Declassification
(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)

$0.00

5. Protection and Maintenance for Classified Information Systems
(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)

$1,500.00

6. Operations Security and Technical Surveillance Countermeasures
(include personnel and operating expenses associated with OPSEC and TSCM)

$0.00

7. Professional Education, Training, and Awareness
(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)

$0.00

8. Security Management, Oversight, and Planning
(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))

$0.00

9. Unique Items
(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)

$0.00

TOTAL
(sum of items 1-9)

$1,333,182.80

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

The amount spent on physical security reflects the growing cost of the headquarters guard contract that is administered by DHS. Personnel Security costs increased due to an increase in agency hiring.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Peace Corps	**Fiscal Year:** 2015

Point of Contact:
(Name and phone number) Nicki Whitaker (202) 692-2553

Reporting Categories

Please use actual dollar figures.

1. Personnel Security
(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)

$296,099.07

2. Physical Security
(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)

$1,100,000.00

3. Classification Management
(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)

4. Declassification
(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)

5. Protection and Maintenance for Classified Information Systems
(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)

6. Operations Security and Technical Surveillance Countermeasures
(include personnel and operating expenses associated with OPSEC and TSCM)

7. Professional Education, Training, and Awareness
(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)

8. Security Management, Oversight, and Planning
(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))

9. Unique Items
(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)

TOTAL
(sum of items 1-9)

$1,396,099.07

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

The amount spent on physical security reflects the cost of the headquarters guard contract that is administered by DHS. Personnel security costs increased by approx. 65K due to an increase in hiring by the agency and the implementation of the new investigative tiers. We now have to utilize OPM for more investigative services.

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified Information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

   1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

   Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

   Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

   National Agency Check: Include only when used for basis for granting a clearance.

   Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

   Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

   Polygraph: Substantive examinations in security screening process.

   2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

   Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

   Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

   Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

   Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION   AUTHORIZED FOR LOCAL REPRODUCTION   STANDARD FORM 716 (07-11)
Page 2 of 4   Prescribed by NARA/ISOO
32 CFR Part 2001.90   E.O. 13526

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. **Classification Management:** The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. **Declassification:** The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. **Protection and Maintenance for Classified Information Systems:** A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. **Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):**

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. **Professional Education, Training, and Awareness:** The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. **Security Management, Oversight, and Planning:** Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION   AUTHORIZED FOR LOCAL REPRODUCTION   STANDARD FORM 716 (07-11)
Page 3 of 4   Prescribed by NARA/ISOO
32 CFR Part 2001.90   E.O. 13526

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. **Unique Items:** Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. **Name of Department/Agency:** Self-explanatory.

2. **Reporting Categories:** List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. **Totals:** The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. **Narrative:** In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION   AUTHORIZED FOR LOCAL REPRODUCTION   STANDARD FORM 716 (07-11)
Page 4 of 4   Prescribed by NARA/ISOO
32 CFR Part 2001.90 E.O. 13526

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Peace Corps	**Fiscal Year:** 2016

Point of Contact:
(Name and phone number) Amelia Sparks, 202-692-2565

Reporting Categories

Please use actual dollar figures.

1. Personnel Security
(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)

$385,191.15

2. Physical Security
(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)

$1,288,555.44

3. Classification Management
(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)

$0.00

4. Declassification
(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)

$0.00

5. Protection and Maintenance for Classified Information Systems
(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)

$30,914.45

6. Operations Security and Technical Surveillance Countermeasures
(include personnel and operating expenses associated with OPSEC and TSCM)

$0.00

7. Professional Education, Training, and Awareness
(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)

$0.00

8. Security Management, Oversight, and Planning
(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))

$0.00

9. Unique Items
(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)

$0.00

TOTAL
(sum of items 1-9)

$1,704,661.04

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

1. PersSec: $214,122.51 FTE staff + $171,068.64 for investigations. I assume that overall increase is due to excluding staff salaries in FY15 for reporting categories 1 & 2. 2. Physical security: $115,555.44 FTE staff + $1,173,000.00 for the guard contract administered by DHS which has a $73,000 increase due to increase in guard hourly wages. 5. Protection & Maintenance: FY16 cost of classified network per the IAA with classified system provider. I do not know why this annual cost was excluded from the FY15 report.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION   AUTHORIZED FOR LOCAL REPRODUCTION   STANDARD FORM 716 (07-11)
Page 1 of 4   Prescribed by NARA/ISOO
32 CFR Part 2001.90 E.O. 13526

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

    1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

        Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

        Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

        National Agency Check: Include only when used for basis for granting a clearance.

        Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

        Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

        Polygraph: Substantive examinations in security screening process.

    2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

        Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

        Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

        Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

        Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION   AUTHORIZED FOR LOCAL REPRODUCTION   STANDARD FORM 716 (07-11)
Page 2 of 4   Prescribed by NARA/ISOO
32 CFR Part 2001.90 E.O. 13526

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. **Classification Management:** The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. **Declassification:** The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. **Protection and Maintenance for Classified Information Systems:** A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. **Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):**

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. **Professional Education, Training, and Awareness:** The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. **Security Management, Oversight, and Planning:** Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. **Unique Items:** Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. **Name of Department/Agency:** Self-explanatory.

2. **Reporting Categories:** List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. **Totals:** The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. **Narrative:** In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION   AUTHORIZED FOR LOCAL REPRODUCTION   STANDARD FORM 716 (07-11)
Page 4 of 4   Prescribed by NARA/ISOO
32 CFR Part 2001.90   E.O. 13526